Introduction

This Reply is in response to the Office Action of January 22, 2009. Reconsideration of this application in view of the following remarks is respectfully requested.

The undersigned thanks the supervising Examiner, Ayaz Sheikh, and the Examiner, Trang T. Doan, for the telephone discussion of May 26, 2009. In the telephone discussion, the undersigned discussed independent claims 1, 13, and 18 and the Response to Arguments section of the Office Action. During the discussion, features of the invention were discussed. The undersigned and the Examiners also discussed the Examiner's position on the prior art that was presented in the Response to Arguments section of the Office Action. Although no agreement was reached on the telephone, applicants believe that the arguments presented below are persuasive and, upon review, will overcome the current rejections.

The Rejections of Claims 1-19

In the Office Action, claims 1-19 were rejected under 35 U.S.C. §102(e) as being anticipated by Zheng (US 6396928). These rejections are respectfully traversed.

Claim 13 is directed to a method of signing and encrypting a message M in which an IBE private key is used to compute a commitment to a secret value and a corresponding decommitment.

In the Response to Arguments section on page 2 of the Office Action, the Patent Office suggested that col. 11, line 25 through col. 12, line 63 and col. 13, lines 20-53 of Zheng disclose using an IBE private key to compute a commitment and a decommitment, as required by claim 13.

However, as the undersigned explained in the May 26, 2009 interview, there is nothing in these portions of Zheng or in any other portion of Zheng that discloses using an IBE private key to compute a commitment and a decommitment.

Because the portions of Zheng that were cited in the January 22, 2009 Office Action fail to show or suggest using an IBE private key to compute a commitment and a decommitment as required by claim 13, claim 13 is patentable over Zheng. Claims 14-17 depend from claim 13 and are patentable because claim 13 is patentable.

Claims 1-12 and 18-19

Claims 1 and 18 are directed to identity-based-encryption signcryption methods in which decrypting a ciphertext

produces an IBE public key of the sender ID_A.

In the Office Action, it was suggested that col. 14, lines 54-67 of Zheng discloses a method in which decryption of ciphertext produces an IBE public key of a sender. However, as the undersigned explained in the May 26, 2009 interview, there is nothing in these portions of Zheng or in any other portion of Zheng that discloses an identity-based-encryption signcryption method in which decrypting a ciphertext produces an IBE public key of the sender ID_A.

Because Zheng fails to show or suggest a method in which decryption of ciphertext produces an IBE public key of a sender of the ciphertext as required by claims 1 and 18, claims 1 and 18 are patentable over Zheng. Claims 2-12 depend from claim 1 and are patentable because claim 1 is patentable. Claim 19 depends from claim 18 and is patentable because claim 18 is patentable.

Conclusion

The foregoing demonstrates that claims 1-19 are in

condition for allowance. Reconsideration and allowance of the

application are respectfully requested.

Respectfully submitted,

Date: May 26, 2009   /David C. Kellogg/
                                      David C. Kellogg
                                      Reg. No. 62,958
                                      Agent for Applicant
                                      Customer No. 36532